IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	CRIMINAL ACTION
v.	:	
	:	NO. 12-0367
DOROTHY JUNE BROWN,	:	
JOAN WOODS CHALKER,	:	
MICHAEL A. SLADE, JR.,	:	
COURTENEY L. KNIGHT	:	

SURRICK, J. **OCTOBER 3, 2013**

MEMORANDUM

Presently before the Court is Defendant Dorothy June Brown's Motion to Suppress Evidence or in the Alternative Request for an Evidentiary Hearing (ECF No. 126). For the following reasons, Defendant's Motion will be denied.

I. BACKGROUND[1]

On January 22, 2013, a federal grand jury returned a sixty-seven count Superseding Indictment against Dorothy June Brown, Joan Woods Chalker, Michael A. Slade, Jr., Courteney L. Knight, and Anthony Smoot. (Superseding Indictment ("Indictment"), ECF No. 47.)[2] These charges arise out of an alleged scheme perpetrated by Brown to defraud three separate charter schools out of over $6.7 million.

[1] The factual background of this case is more fully set forth in the Court's June 19, 2013 Memorandum denying Defendant Joan Woods Chalker's Motion to Dismiss Wire Fraud Counts 15 through 37 and Defendant Dorothy June Brown's Motion to Dismiss Counts 1 through 37 of the Superseding Indictment or in the Alternative, Motion to Strike the Conflict of Interest Allegations and/or Motion for a Bill of Particulars. (*See* ECF No. 122.)

[2] On March 15, 2013, Anthony Smoot entered a guilty plea to conspiracy to obstruct justice, in violation of 18 U.S.C. § 371 (Count 53), and obstruction of justice, in violation of 18 U.S.C. § 1519 and § 2 (Count 58). (Min. Entry, ECF No. 55.) His sentencing is scheduled for December 3, 2013. (ECF No. 103.)

The Indictment charges Brown with fifty-two counts of wire fraud, in violation of 18 U.S.C. § 1343 (Counts 1-52), one count of conspiring to obstruct justice, in violation of 18 U.S.C. § 371 (Count 53), ten counts of obstruction of justice, in violation of 18 U.S.C. § 1519 (Counts 54-59, 63, 65) and § 1512(c)(2) (Counts 61-62), and one count of witness tampering, in violation of 18 U.S.C. § 1512(b)(3) (Count 67).

A. Factual Background

1. The Warrant, Search and Seizure

On May 6, 2010, agents from the Federal Bureau of Investigations ("FBI") and the United States Department of Education, Office of the Inspector General ("ED/OIG") executed a search of 124 Bryn Mawr Avenue, Bala Cynwyd, Pennsylvania, the administrative offices of Brown's schools and other businesses. The search was conducted pursuant to a Search Warrant issued by United States Magistrate Judge R. Felipe Restrepo on May 4, 2010. (Warrant, Def.'s Mot. Ex. B, ECF No. 127.) The Warrant application was supported by an Affidavit furnished by Kristy Smith, a Special Agent with the ED/OIG. (Warrant Attach. B.) The Warrant authorized the search and seizure of the following materials:

> 1. All records and documents pertaining to federal grants and other federal funding administered by any federal, state, or local agency, including the United States Department of Education, the Pennsylvania Department of Education, and the School District of Philadelphia.
>
> 2. All records and documents that reflect the receipt, use, or transfer of money or other assets belonging to Agora Cyber Charter School, Main Line Academy, Ad Prima Charter School, Planet Abacus Charter School, Laboratory Charter School, The Cynwyd Group, Main Line Academic Services, Inc., Academic Quest, LLC, and Educational Services (collectively, "The BROWN ENTITIES,") including books, receipts, ledgers, account statements, money drafts, money orders, letters of credit, cashier checks, passbooks, bank checks, accounts receivable journals, accounts payable journals, contracts, vendor files, tax records, credit card statements, travel itineraries, vehicle lease agreements, property lease agreements, insurance policies, and loan records.

3. All correspondence that pertains to the receipt, use, or transfer of money or other assets belonging to the BROWN ENTITIES, including electronic mail, board minutes, memoranda, notes, reports, summaries, offers, inquiries, bulletins, newsletters, charts, graphs, articles, announcements, books, and audio and video recordings.

4. All Rolodex files, appointment books, notes, calendars, diaries, and journals belonging to the BROWN ENTITIES, or their officers, employees, or contractors.

5. All records and documents concerning vehicles owned or leased by the BROWN ENTITIES, or any of their officers, employees, or contractors.

6. All personnel records and documents for officers, employees, and contractors of the BROWN ENTITIES, including student employees, including records and documents regarding payroll, benefits, and professional development, and statements of financial interests, timesheets, applications for employment, and job descriptions.

7. All employee handbooks, manuals, or policies of the BROWN ENTITIES.

8. All records and documents relating to U.S. Post Office Boxes, private mail boxes, storage lockers, safes, and safety deposit boxes rented or owned by the BROWN ENTITIES, or their officers, employees, or contractors.

9. Computers and computer-related equipment containing the records identified in paragraphs 1-8 above, including any and all information, instructions, programs and/or data stored in the form of magnetic, electronic, optical, or other coding on computer media or on media capable of being read by a computer or with the aid of computer related equipment. This media includes but is not limited to disks/diskettes, flash cards, cartridges, tapes, optical medium, hard disk drives, solid-state devices and any other media that are capable of storing information or data.

    a. This further includes any and all electronic devices which are capable of analyzing, creating, displaying, converting, storing, or transmitting electronic, magnetic, or optical computer impulses or data, and any manuals or software relating to such devices. These devices include but are not limited to computers, computer components, computer peripherals, modems, monitors, speakers, printers, scanners, cameras, cell phones, personal digital assistants (pda's), MP3 audio players, wireless devices, Universal Serial Bus (USB) devices, Firewire devices and networking equipment; and
    b. Any and all software plus the manuals or instructions relating to such software as is used by the electronic devices or media previously specified in this attachment.

The Government seized 160 items, including 22 computer hard drives, 51 thumb drives, approximately 130 boxes of paper documents, and other digital media devices. (Evidence Inventory Form, Def.'s Mot. Ex. C; Gov't's Resp. 7, ECF No. 130.)[3] After seizing these materials, the Government retained the services of the Philadelphia Regional Computer Forensics Laboratory ("PRCFL") to conduct forensic examinations of the materials. (Def.'s Mot. 5.) Forensic examiners imaged the computers, thumb drives, and other media, and each piece of digital media was assigned a "QPH" number for reference. (Gov't's Resp. 6; June 22 Report 7, Def.'s Mot. Ex. D.) As detailed in the December 9, 2010, PRCFL Report, the federal agents submitted keyword search lists to the forensic examiners in order to search the data. (Gov't's Resp. 6.) The Government has not disclosed to Defendants the keyword phrases used for this search. Approximately 75,000 documents were identified as a result of the keyword search. (*Id.* at 6 n.5.) These documents were then imported into the Government's database for manual review. (*Id*.)

Agents also manually reviewed data from twenty thumb drives ("Chalker thumb drives") recovered from 124 Bryn Mawr Avenue. Agents selected approximately 1,800 documents from the thumb drives that they found relevant and within the scope of the warrant. These documents were imported on to an electronic disk. (*Id*.)

Finally, Agents reviewed the materials from the 130 boxes of paper documents recovered from Brown's administrative offices. The agents selected approximately 2,100 documents from those paper records. (*Id*. at 7.)

[3] In total, the Government estimates that it recovered 99 digital media storage devices. (Gov't's Resp. 6 n.5.)

The Government then created an electronic database, referred to by both parties as the "Government Subset," which contains the approximately 78,800 documents that were selected based on the aforementioned searches of the materials recovered from 124 Bryn Mawr Avenue. (*Id*.) The Government Subset was then provided to Defendants and included all available load files, metadata, and database information. (*Id*.)

In 2012, another forensic search was conducted on ninety-nine media storage devices. (Def.'s Mot. 8; Gov't's Resp. 7 n.6.) This search involved the use of twenty-nine specific phrases that agents located during their review of contracts, board minutes, and correspondence. (Gov't's Resp. 7 n.6.) The search terms used during this 2012 search resulted in the identification of twenty-two documents. These search terms were disclosed to Defendants.

B. Procedural History

On July 29, 2013, Defendant filed the instant Motion to Suppress Evidence, or in the Alternative Request for an Evidentiary Hearing. (Def.'s Mot.) The Government submitted a response on August 13, 2013. (Gov't's Resp.) On September 6, 2013, oral argument was held on the Motion. (Min. Entry, ECF No. 140.) At oral argument, Defendant argued for the first time that certain documents were improperly seized as a result of the use of broad search terms. (Sept. 6 Hr'g Tr. 25-28; *see also* Def.'s Sept. 23, 2013 Ltr. (on file with Court).) Specifically, Defendant submitted an exhibit at the oral argument ("Exhibit T"), which listed 265 documents by bates-stamp number. Defendant contends that these documents were improperly seized. (Sept. 6 Hr'g Tr. 25-26 & Ex. T.) Defendant did not provide the Court with a copy of these documents or a description of these documents. The Government advised the Court that it would review the 265 documents, and respond to Defendant's argument. (*Id*. at 38-39.) Defendant also raised for the first time at oral argument an objection that the Government's

search and seizure of documents interfered with Defendant's right to attorney-client privilege. (*Id*. at 25.)

On September 23, 2013, counsel for Defendant sent a letter to the Court reiterating Defendant's request for an evidentiary hearing. (Def.'s Sept. 23, 2013 Ltr. (on file with Court).) The purpose of the hearing would be to require the Government to (1) present evidence regarding the procedures it used to ensure privileged materials were not seized; (2) produce the key word searches used during the 2010 forensics analysis of the electronic documents; and (3) present a witness who would testify about the manual review of the documents contained on the Chalker Thumb Drive.

On September 24, 2013, the Government filed a Supplemental Response to Defendant's Motion. (Gov't's Supp. Resp., ECF No. 144.)

II. DISCUSSION

A. Parties' Contentions

Defendant contends that the Government did not properly limit its search to the categories listed in the warrant and, as a result, all files seized in the search and any evidence derived therefrom must be suppressed. (Def.'s Mot. 18-19.)[4] Defendant has identified 265 documents pulled from the Government's Subset that, in her estimation, fall outside the scope of the Warrant and must be suppressed. (Hr'g Tr. 25; Ex. T (on file with Court).)[5] Moreover, Defendant contends that some of these illegally seized documents were used in the

[4] At argument on the Motion, Defendant asserted that she did not seek suppression of all evidence. Rather, she seeks suppression of any evidence improperly seized. (Sept. 6, 2013, Hr'g Tr. 3 (on file with Court).)

[5] Defendant presented Exhibit T to the Court and the Government at the oral argument. Exhibit T consists of a list of the documents Defendant considers outside the scope of the warrant. Defendant did not provide the Court or the Government with the actual documents.

Government's investigation in the interviews of witnesses. (Hr'g Tr. 26-27.) Defendant requests that the Court hold an evidentiary hearing to fully develop the record on the process used by the Government to search the electronic data. (Def.'s Mot. 21-22.)

The Government responds that it properly searched the electronically stored information for documents that fell within the scope of the Warrant, and, as such, neither an evidentiary hearing nor suppression of any evidence is warranted. (Gov't's Resp. 8.)

B. Legal Standard

1. Fourth Amendment: Search and Seizure

The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. It further provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." *Id.*; *see also United States v. Christine*, 687 F.2d 749, 752 (3d Cir. 1982). Defendant does not challenge the validity of the warrant or claim that the Government lacked probable cause. Rather, Defendant contends that the Government improperly searched Defendant's electronic storage devices and seized material outside the scope of the warrant.

"'[A] seizure lawful at its inception can nevertheless violate the Fourth Amendment if its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on unreasonable seizures.'" *United States v. Stabile*, 633 F.3d 219, 235 (3d Cir. 2011) (quoting *United States v. Jacobsen*, 466 U.S. 109, 124 (1984)). It is well settled that "[i]f the scope of the search exceeds that permitted by the terms of a validly issued warrant . . . the subsequent seizure is unconstitutional without more." *Horton v. California*, 496 U.S. 128, 140 (1990). The defendant bears the burden of establishing that her Fourth

Amendment rights were violated by the challenged search or seizure. *Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978).

2. Evidentiary Hearing

Federal Rule of Criminal Procedure 12(b)(3)(C) provides that a defendant is permitted to file a motion to suppress evidence prior to the start of trial. The Court "may" schedule a hearing on the motion, but an evidentiary hearing on a motion to suppress is not granted as a matter of course. *United States v. Hines*, 628 F.3d 101, 105 (3d Cir. 2010) (citing Fed. R. Crim. P. 12(c)). The Court is required to hold a hearing if the defendant's motion is "sufficiently specific, non-conjectural, and detailed to enable the court to conclude that (1) the defendant has presented a colorable constitutional claim, and (2) there are disputed issues of material fact that will affect the outcome of the motion to suppress." *Id*. (citing *United States v. Voigt*, 89 F.3d 1050, 1067 (3d Cir. 1996)). "[T]he purpose of an evidentiary hearing in the context of a suppression motion is to assist the court in ruling upon a defendant's specific allegations of unconstitutional conduct—its purpose is not to assist the moving party in making discoveries that, once learned, might justify the motion after the fact." *Id*.

In order to raise a constitutional claim in a motion to suppress evidence, the defendant must identify a violation that occurred and "allege facts that, if true, would support a finding that the evidence in question was obtained in violation of the defendant's constitutional rights." *Id.* at 105-06. A defendant may raise an issue of material fact by "submitting evidence that, if true, would tend to establish an essential element of his or her claim that evidence was obtained unconstitutionally." *Id*. at 106.

C. Analysis

1. The Government's Search Was Proper

Defendant challenges the execution of the Search Warrant, claiming that the Government conducted an unconstitutional general search by seizing and reviewing documents beyond the categories enumerated in the Warrant. The issues presented by Defendant here require the Court to wade into an ever-evolving area of law—the Fourth Amendment in the context of computer searches. With the advent of the computer era, and the search of electronic storage devices becoming a commonplace occurrence in criminal investigations, courts have grappled with the balance between a defendant's privacy interest and legitimate law-enforcement concerns in the search of these devices.

The Third Circuit, in the case of *United States v. Stabile*, recently had occasion to address the issue of the Fourth Amendment in the context of computer searches. In *Stabile,* the Government seized six computer hard drives in connection with an investigation into counterfeit checks. 633 F.3d at 224-25. The defendant challenged the Government's seizure noting that by seizing the hard drives, the Government also sized personal emails and other information unrelated to the financial crimes under investigation. *Id*. at 233-34. The court determined that the seizure of the entirety of the hard drives was perfectly reasonable because "evidence of financial crimes could have been found in any location on any of the six hard drives, and this evidence very likely would have been disguised or concealed somewhere on the hard drive." *Id*. at 234. The court also recognized that during reviews of a large cache of documents "'it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.'" *Id.* (quoting *Andersen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)).

The defendant in *Stabile* also challenged the search methodology used by the law enforcement official who searched the hard drives. During the search of the hard drives, the detective opened and reviewed a folder that contained child pornography. The defendant argued this was an "unreasonably overbroad search," which was "not limited to evidence of financial crimes." *Id.* at 237. The Third Circuit expressly disagreed, holding that the detective's decision to view the contents of the folder was "objectively reasonable because criminals can easily alter file names and file extensions to conceal contraband." *Id.* at 239. The Third Circuit recognized that other circuit courts of appeals had authorized at least a "'cursory review of each file on the computer'" *id.* (quoting *United States v. Williams*, 592 F.3d 511, 522 (4th Cir. 2010), and that "'there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders'" while conducting an electronic search. *Id.* (quoting *United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009). Ultimately, the court concluded that the detective's search complied with the warrant and that he conducted a focused search of the hard drives, rather than a general search. *Id.* at 239-40.

Here, Defendant contends that the Government conducted a general search by accessing or viewing every document recovered from 124 Bryn Mawr Avenue. Defendant is simply wrong. The Third Circuit in *Stabile*, explicitly acknowledged that the Government's broad seizure and review of six hard drives was reasonable as "evidence of financial crimes could have been found in any location on any of the six hard drives, and this evidence very likely would have been disguised or concealed somewhere on the hard drive." *Id*. at 234. Other circuits agree that a broad search of computer files is reasonable in light of the nature of searching electronic documents. *See Burgess*, 576 F.3d at 1094 (stating that "there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within

those folders, and that is true whether the search is of computer files or physical files"); *United States v. Richards*, 659 F.3d 527, 536-40 (6th Cir. 2011) ("[S]o long as the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officers to open the various types of files located in the computer's hard drive in order to determine whether they contain such evidence."); *Williams*, 592 F.3d at 523 (concluding that agents conducting search were authorized to cursorily open each filed on the computer and view its contents); *see also United States v. Fumo*, No 06-319, 2007 WL 3232112, at *6 (E.D. Pa. Oct. 30, 2007) ("Regardless of the search protocols or keywords used by the government, the government may open and briefly examine each computer file to determine whether it is within the description recited in the warrant."). The Government's search of the computer and other electronic media files in this case was entirely proper.

2. The Government's Seizure was Proper, and an Evidentiary Hearing Is Not Required.

Defendant also contends that the Government's seizure of documents exceeded the scope of the warrant.[6] In particular, Defendant takes issue with the 265 documents seized that she contends (1) fell outside the scope of the warrant, and (2) demonstrate that the search procedures used by the Government were improper. Defendant claims that these documents were used by the Government to interview witnesses during its investigation of this case.[7] Based upon this

[6] The Government seized approximately 160 items, including hard drives, thumb drives, and other electronic storage media devices. Out of these 160 items, the Government pulled over 78,000 documents that it found relevant and within the scope of the warrant. In order to determine whether or not these documents were within the scope of the warrant, the Government was entitled to open and briefly examine every computer file. *See supra* Section II.C.1.

[7] Defendant identified a total of six witnesses who she claims were interviewed using documents from outside the scope of the warrant. (Hr'g Tr. 26-27.) She asserts that upon review of the 302 reports of the agents' interviews, it was apparent that the agents were referencing documents which fell beyond the scope of the warrant. (*Id*. at 48-49.)

belief, Defendant requests an evidentiary hearing, the purpose of which would be to, among other purposes, require the Government to "produce the keyword search terms used in the review process . . . on November 10, 2010" and "present a witness who can testify why the selected search terms were expected to properly identify . . . information within the scope of the search warrant." (Def.'s Sept. 23 Ltr 1.)

In its Supplemental Response, the Government advised that none of the 265 documents identified by Defendant were shown to witnesses or used in any way during the Government's investigation into this matter. (Gov't's Supp. Resp. 13.) The Government specifically states that "[it] has reviewed the interview reports and grand jury testimony of the individuals named at the hearing," and that "[n]one of those individuals were shown any of the 265 'QPH' documents listed on defendant Brown's September 6th disclosure." (*Id.*) Defendant has not filed a reply disputing the Government's representation with regard to the 265 documents. Moreover, Defendant has not submitted an affidavit from any of those individuals who were allegedly interviewed in support of her contention. Defendant has failed to demonstrate that any one of the 265 documents was seized outside the scope of the warrant. Defendant's failure to allege a factual dispute or wrongdoing on the part of the Government with any specificity is fatal to her request for an evidentiary hearing. *See Hines*, 628 F.3d at 105 (conditioning a grant of an evidentiary hearing on a defendant's ability to demonstrate with sufficient non-conjectural specificity (1) a colorable constitutional claim and (2) disputed issues of material fact); *Voight*, 89 F.3d at 1067 (noting that to be "colorable," a claim must contain more than "bald-faced allegations of misconduct."); *United States v. Jackson*, 363 F. App'x 208, 210 n.2 (3d Cir. 2010)

(stating that "in order to receive a pretrial evidentiary hearing," there must be "significant factual disputes").

Defendant has failed to meet her burden in demonstrating that a pretrial evidentiary hearing is required. Defendant has simply made bald accusations and assertions. This is not sufficient. We are therefore compelled to deny her request. *See United States v. Sepling*, No. 11-195, 2012 WL 1356714, at *6 n.2 (M.D. Pa. April 19, 2012) (denying the defendant's motion to suppress and request for an evidentiary hearing where the defendant failed to identify facts material to his claim and failed to refuse the Government's version of events). *C.f. United States v. Judge*, 447 F. App'x 409, 414 n.8 (3d Cir. 2011) (affirming district court's denial of evidentiary hearing where the defendant "failed to put forth any factual challenge" to the facts developed at a state court proceeding surrounding his motion to suppress statements).

Nor is Defendant entitled to a hearing simply to obtain the search terms used by the Government in 2010. In *Fumo*, the court held that "[t]he search protocols and keywords used by the government are irrelevant to the decision whether the warrants were overbroad or the seizures exceeded the scope of the warrants." 2007 WL 3232112, at *5. In a comprehensive and well-reasoned analysis, the court concluded that information related to search protocols and keywords is not necessary to analyze whether evidence seized pursuant to a warrant should be suppressed beacuse suppression can be determined from the face of the warrant, and any evidence falling outside of the scope of the warrant can be excluded. *Id*. We agree. Defendant attempts to distinguish *Fumo* by contending that, unlike the facts presented here, the defendant in *Fumo* did not present evidence that the Government's searches had in fact produced documents that fell outside the scope of the warrant. (Def.'s Mot. 22 n.6.) Defendant's argument is unavailing. As noted above, Defendant has failed to identify with specificity one relevant

document that she contends fell outside the scope of the warrant. The Government is under no obligation to produce the keyword phrases it used in its 2010 forensic analysis.

Finally, Defendant requests a hearing for the purpose of requiring the Government to "present evidence that it established and implemented procedures to ensure privileged materials were properly segregated from the information seized during the search warrant and subsequently reviewed by the investigating agents." (Def.'s Sept. 23 Ltr. 1.) At the September 6, 2013 oral argument, Defendant for the first time raised concerns that during its search and seizure of documents, the Government invaded Defendant's right to attorney-client privilege. Specifically, Defendant contends that the Government delegated its privilege review to agents who are not attorneys and who are not trained in recognizing what information constitutes privileged information. (Sept. 6 Hr'g Tr. 24-25.) In response, the Government explains that a privilege review was conducted, and that, in fact, the review was completed by an attorney. (*Id.* at 44-45.) The Government points out that in September of 2012, it discussed with defense counsel the privilege review process and a protocol was adopted by agreement. Under that protocol, a taint team attorney conducted the privilege review and kept defense counsel advised. (Gov't's Supp. Resp. 14-17.) In addition, the Government argues that Defendant has failed to identify any seized documents that are subject to the attorney-client privilege, and has thus failed to show that the privilege was in fact invaded. (Gov't's Supp. Resp. 14-15.) Defendant presents only a speculative basis in support of her request without any specificity. She has failed to meet her burden in demonstrating that she is entitled to an evidentiary hearing to probe the attorney-client privilege review process undertaken by the Government. *See United States v. SDI Future Health, Inc.*, 464 F. Supp. 2d 1027, 1055 (D. Nev. 2006) (denying the defendant's request for an evidentiary hearing to address the Government's alleged violation of the attorney-client privilege

where the defendant failed to demonstrate that the prosecution had access to any privileged documents). Defendant's request for an evidentiary hearing will be denied.

IV. CONCLUSION

For the foregoing reasons, Defendant's Motion to Suppress Evidence or in the Alternative Request for an Evidentiary Hearing will be denied.

An appropriate Order follows.

BY THE COURT:

/s/R. Barclay Surrick
U.S. District Judge